Three things you can do today to test your HR resilience

Net-Defence
Ogilvie House, Princes Park, Team Valley Trading Estate, Gateshead NE11 0NF • Ogilvie House, 200 Glasgow Road, Stirling FK7 SES
Tel: 03300 241 666 • Web: net-defence.com

Short resilience tests are effective because they reveal the reality quickly. They cut through assumptions and highlight vulnerabilities in minutes that a formal audit might take months to uncover. While audits assess what policies and processes should look like, short tests show what actually happens in practice, under real conditions with real people.

They provide clear, actionable insights without the cost, complexity or time commitment of a full review. In an environment where HR disruption can quickly ripple across an organisation, these quick checks are not a luxury, they're an essential part of maintaining resilience.

Here are three practical examples:

1. Run a 10 minute 'HR offline' scenario

Ask the simple question: If HR systems were unavailable for the next 48 hours, what stops working immediately? Consider:

Operational processes

- Can you still run payroll changes?
- Can onboarding or offboarding continue securely?
- Are managers able to safely access the policies and documents they need, without bypassing process?

People management & governance processes

- What happens to active grievances?
- What happens to ongoing disciplinary cases?
- Who manages investigations, welfare meetings, or factfinding if HR isn't available?
- Are managers equipped and authorised to step in temporarily without compromising compliance or fairness?

Welfare & support

- Who picks up employee wellbeing concerns, sickness management, or urgent welfare issues?
- Is there a fallback route employees can use if they need HR support, but the function is offline?
- Is that fallback secure, documented and traceable?

This exposes operational dependencies, single points of failure, and undocumented workarounds faster than any audit.

2. Test how easy it is to make a HR data mistake

This is the most common breach area, and the easiest to test. Here's what to do in practice:

- Draft an email with an attachment containing placeholder 'employee data.'
- Add a distribution list and a few similar looking names.
- Ask HR to identify the risk points and what controls (technical and behavioural) would catch the error.

If the only thing preventing a mistake is relying on people to 'be careful' rather than having technical controls (like automated checks, permissions) or behavioural safeguards (like double-checks, approval processes), then there's a real risk that someone could make a mistake and sensitive data could be exposed.

3. Review current access permissions immediately

Access drift is one of HR's biggest weaknesses. Ask your IT/HR leads to generate a quick list of:

- Who currently has access to HR systems
- Who has access to employee records
- Who used to have access but no longer should
- Whether access is role based or carried over from years ago

You will almost certainly uncover dormant accounts, unnecessary access, or legacy permissions – all red flags for both internal misuse and external compromise.

These are situations where HR's absence creates risk rapidly. These tests quickly expose:

- Single points of failure
- Gaps in documentation
- Overreliance on individual HR team members
- Vulnerable welfare and governance processes
- Whether the business would default to informal, undocumented workarounds

If you want to learn more about how to test your HR resilience, **get in touch with us today** for expert advice and practical guidance.